NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27001

Segunda edição
08.11.2013

Válida a partir de
08.12.2013

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos

Information technology — Security techniques — Information security management systems — Requirements

ICS 35.040

ISBN 978-85-07-04608-0

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27001:2013
30 páginas

© ISO/IEC 2013 - © ABNT 2013

© ISO/IEC 2013
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT, único representante da ISO no território brasileiro.

© ABNT 2013
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT.

ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Sumário

Página

Prefácio Nacional iv
0 Introdução v
0.1 Geral v
0.2 Compatibilidade com outras normas de sistemas de gestão v
1 Escopo 1
2 Referência normativa 1
3 Termos e definições 1
4 Contexto da organização 1
4.1 Entendendo a organização e seu contexto 1
4.2 Entendendo as necessidades e as expectativas das partes interessadas 1
4.3 Determinando o escopo do sistema de gestão da segurança da informação 2
4.4 Sistema de gestão da segurança da informação 2
5 Liderança 2
5.1 Liderança e comprometimento 2
5.2 Política 3
5.3 Autoridades, responsabilidades e papéis organizacionais 3
6 Planejamento 3
6.1 Ações para contemplar riscos e oportunidades 3
6.1.1 Geral 3
6.1.2 Avaliação de riscos de segurança da informação 4
6.1.3 Tratamento de riscos de segurança da informação 5
6.2 Objetivo de segurança da informação e planejamento para alcançá-los 5
7 Apoio 6
7.1 Recursos 6
7.2 Competência 6
7.3 Conscientização 6
7.4 Comunicação 7
7.5 Informação documentada 7
7.5.1 Geral 7
7.5.2 Criando e atualizando 7
7.5.3 Controle da informação documentada 7
8 Operação 8
8.1 Planejamento operacional e controle 8
8.2 Avaliação de riscos de segurança da informação 8
8.3 Tratamento de riscos de segurança da informação 8
9 Avaliação do desempenho 9
9.1 Monitoramento, medição, análise e avaliação 9
9.2 Auditoria interna 9
9.3 Análise crítica pela Direção 10
10 Melhoria 10
10.1 Não conformidade e ação corretiva 10

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

10.2 Melhoria contínua.....11
Bibliografia 30

Anexo
Anexo A (normativo) **Referência aos controles e objetivos de controles 12**

Tabela
Tabela A.1 – Objetivos de controle e controles 12

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretiva ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO/IEC 27001 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00). O Projeto circulou em Consulta Nacional conforme Edital nº 09, de 26.09.2013 a 25.10.2013, com o número de Projeto ABNT NBR ISO/IEC 27001.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27001:2013, que foi elaborada pelo *Technical Committee Information Technology* (ISO/IEC JTC 1), *Subcommittee Security Techniques* (SC 27), conforme ISO/IEC Guide 21-1:2005.

Esta segunda edição cancela e substitui a edição anterior (ABNT NBR ISO/IEC 27001:2006), a qual foi tecnicamente revisada.

O Escopo desta Norma Brasileira em inglês é o seguinte:

Scope

This Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this Standard.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

0 Introdução

0.1 Geral

Esta Norma foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo.

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que um sistema de gestão da segurança da informação seja parte de, e esteja integrado com, os processos da organização e com a estrutura de administração global, e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles. É esperado que a implementação de um sistema de gestão de segurança da informação seja planejada de acordo com as necessidades da organização.

Esta Norma pode ser usada por partes internas e externas, para avaliar a capacidade da organização em atender aos seus próprios requisitos de segurança da informação.

A ordem na qual os requisitos são apresentados nesta Norma não reflete sua importância nem implica a ordem em que devem ser implementados. Os itens listados são numerados apenas para fins de referência.

A ISO IEC 27000 descreve a visão geral e o vocabulário do sistema de gestão da segurança da informação e referência às normas da família do sistema de gestão da segurança da informação (incluindo a ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), com termos e definições relacionados.

0.2 Compatibilidade com outras normas de sistemas de gestão

Esta Norma aplica a estrutura de alto nível, os títulos de subseções idênticos, textos idênticos, termos comuns e definições básicas, apresentadas no Anexo SL da ISO/IEC *Directives*, Part 1, *Consolidated ISO Supplement*, mantendo desta forma a compatibilidade com outras normas de sistemas de gestão que adotaram o Anexo SL.

Esta abordagem comum definida no Anexo SL será útil para aquelas organizações que escolhem operar um único sistema de gestão que atenda aos requisitos de duas ou mais normas de sistemas de gestão.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos

1 Escopo

Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos definidos nesta Norma são genéricos e são pretendidos para serem aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. A exclusão de quaisquer dos requisitos especificados nas Seções 4 a 10 não é aceitável quando a organização busca a conformidade com esta Norma.

2 Referência normativa

O documento relacionado a seguir é indispensável à aplicação deste documento. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições apresentados na ISO/IEC 27000.

4 Contexto da organização

4.1 Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

NOTA A determinação destas questões refere-se ao estabelecimento do contexto interno e externo da organização apresentado em 5.3 da ABNT NBR ISO 31000:2009 [5].

4.2 Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação; e

b) os requisitos dessas partes interessadas relevantes para a segurança da informação.

NOTA Os requisitos das partes interessadas podem incluir requisitos legais e regulamentares, bem como obrigações contratuais.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

4.3 Determinando o escopo do sistema de gestão da segurança da informação

A organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer o seu escopo.

Quando da determinação deste escopo, a organização deve considerar:

a) as questões internas e externas referenciadas em 4.1;

b) os requisitos referenciados em 4.2; e

c) as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas que são desempenhadas por outras organizações.

O escopo deve estar disponível como informação documentada.

4.4 Sistema de gestão da segurança da informação

A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação, de acordo com os requisitos desta Norma.

5 Liderança

5.1 Liderança e comprometimento

A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização;

b) garantindo a integração dos requisitos do sistema de gestão da segurança da informação dentro dos processos da organização;

c) assegurando que os recursos necessários para o sistema de gestão da segurança da informação estão disponíveis;

d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;

e) assegurando que o sistema de gestão da segurança da informação alcança seus resultados pretendidos;

f) orientando e apoiando pessoas que contribuam para eficácia do sistema de gestão da segurança da informação;

g) promovendo a melhoria contínua; e

h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

5.2 Política

A Alta Direção deve estabelecer uma política de segurança da informação que:

a) seja apropriada ao propósito da organização;

b) inclua os objetivos de segurança da informação (ver 6.2) ou forneça a estrutura para estabelecer os objetivos de segurança da informação;

c) inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;

d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política de segurança da informação deve:

a) estar disponível como informação documentada;

b) ser comunicada dentro da organização; e

c) estar disponível para as partes interessadas, conforme apropriado.

5.3 Autoridades, responsabilidades e papéis organizacionais

A Alta Direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

A Alta Direção deve atribuir a responsabilidade e autoridade para:

a) assegurar que o sistema de gestão da segurança da informação está em conformidade com os requisitos desta Norma;

b) relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção.

NOTA A Alta Direção pode também atribuir responsabilidades e autoridades para relatar o desempenho do sistema de gestão da segurança da informação dentro da organização.

6 Planejamento

6.1 Ações para contemplar riscos e oportunidades

6.1.1 Geral

Quando do planejamento do sistema de gestão da segurança da informação, a organização deve considerar as questões referenciadas em 4.1 e os requisitos descritos em 4.2 e determinar os riscos e oportunidades que precisam ser consideradas para:

a) assegurar que o sistema de gestão da segurança da informação pode alcançar seus resultados pretendidos;

b) prevenir ou reduzir os efeitos indesejados; e

c) alcançar a melhoria contínua.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

A organização deve planejar:

a) as ações para considerar estes riscos e oportunidades; e

b) como

   1) integrar e implementar estas ações dentro dos processos do seu sistema de gestão da segurança da informação; e

   2) avaliar a eficácia destas ações.

6.1.2 Avaliação de riscos de segurança da informação

A organização deve definir e aplicar um processo de avaliação de riscos de segurança da informação que:

a) estabeleça e mantenha critérios de riscos de segurança da informação que incluam:

   1) os critérios de aceitação do risco; e

   2) os critérios para o desempenho das avaliações dos riscos de segurança da informação;

b) assegure que as contínuas avaliações de riscos de segurança da informação produzam resultados comparáveis, válidos e consistentes;

c) identifique os riscos de segurança da informação:

   1) aplicando o processo de avaliação do risco de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação; e

   2) identificando os responsáveis dos riscos.

d) analise os riscos de segurança da informação:

   1) avalie as consequências potenciais que podem resultar se os riscos identificados em 6.1.2 c) 1) forem materializados

   2) avalie a probabilidade realística da ocorrência dos riscos identificados em 6.1.2 c) 1); e

   3) determine os níveis de risco;

e) avalie os riscos de segurança da informação:

   1) compare os resultados da análise dos riscos com os critérios de riscos estabelecidos em 6.1.2 a); e

   2) priorize os riscos analisados para o tratamento do risco.

A organização deve reter informação documentada sobre o processo de avaliação de risco de segurança da informação.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

6.1.3 Tratamento de riscos de segurança da informação.

A organização deve definir e aplicar um processo de tratamento dos riscos de segurança da informação para:

a) selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco;

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação;

NOTA As organizações podem projetar os controles, conforme requerido, ou identificá-los de qualquer outra fonte.

c) comparar os controles determinados em 6.1.3 b) com aqueles do Anexo A e verificar se algum controle necessário foi omitido;

NOTA 1 O Anexo A contém uma lista detalhada dos controles e dos objetivos de controle. Os usuários desta Norma são instruídos a utilizar o Anexo A para garantir que nenhum controle necessário seja omitido;

NOTA 2 Os objetivos de controle estão implicitamente incluídos nos controles escolhidos. Os objetivos de controle e os controles listados no Anexo A não são exaustivos, e controles e objetivos de controles adicionais podem ser necessários.

d) elaborar uma declaração de aplicabilidade que contenha os controles necessários (ver 6.1.3 b) e c)), e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles do Anexo A;

e) preparar um plano para tratamento dos riscos de segurança da informação; e

f) obter a aprovação dos responsáveis pelos riscos do plano de tratamento dos riscos de segurança da informação e a aceitação dos riscos residuais de segurança da informação.

A organização deve reter a informação documentada relativa ao processo de tratamento dos riscos de segurança da informação.

NOTA O processo de tratamento e a avaliação dos riscos de segurança da informação desta Norma estão alinhados com os princípios e diretrizes gerais definidos na ABNT NBR ISO 31000 [5].

6.2 Objetivo de segurança da informação e planejamento para alcançá-los

A organização deve estabelecer os objetivos de segurança da informação para as funções e níveis relevantes.

Os objetivos de segurança da informação devem:

a) ser consistentes com a política de segurança da informação;

b) ser mensuráveis (quando aplicável);

c) levar em conta os requisitos de segurança da informação aplicáveis e os resultados da avaliação e tratamento dos riscos;

d) ser comunicados; e

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

e) ser atualizados, conforme apropriado.

A organização deve reter informação documentada dos objetivos de segurança da informação.

Quando do planejamento para alcançar os seus objetivos de segurança da informação, a organização deve determinar:

a) o que será feito;

b) quais recursos serão necessários;

c) quem será responsável;

d) quando estará concluído;

e) como os resultados serão avaliados

7 Apoio

7.1 Recursos

A organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação.

7.2 Competência

A organização deve:

a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;

b) assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados;

c) onde aplicável, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e

d) reter informação documentada apropriada como evidência da competência.

NOTA Ações apropriadas podem incluir, por exemplo: fornecimento de treinamento para os facilitadores, os funcionários atuais ou pessoas competentes, próprias ou contratadas.

7.3 Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

a) política de segurança da informação;

b) suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

c) implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

7.4 Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão da segurança da informação incluindo:

a) o que comunicar;

b) quando comunicar;

c) quem comunicar;

d) quem será comunicado; e

e) o processo pelo qual a comunicação será realizada.

7.5 Informação documentada

7.5.1 Geral

O sistema de gestão da segurança da informação da organização deve incluir:

a) informação documentada requerida por esta Norma;

b) informação documentada determinada pela organização como sendo necessária para a eficácia do sistema de gestão da segurança da informação.

NOTA A abrangência da informação documentada para o sistema de gestão da segurança da informação pode variar de uma organização para outra devido:

1) ao tamanho da organização e seu tipo de atividades, processos, produtos e serviços;

2) à complexidade dos processos e suas interações;

3) à competência das pessoas.

7.5.2 Criando e atualizando

Quando da criação e atualização da informação documentada, a organização deve assegurar, de forma apropriada:

a) identificação e descrição (por exemplo, título, data, autor ou um número de referência);

b) formato (por exemplo, linguagem, versão do software, gráficos) e o seu meio (por exemplo, papel, eletrônico); e

c) análise crítica e aprovação para pertinência e adequação.

7.5.3 Controle da informação documentada

A informação documentada requerida pelo sistema de gestão da segurança da informação e por esta Norma deve ser controlada para assegurar que:

a) esteja disponível e adequada para o uso, onde e quando necessário;

b) esteja protegida adequadamente (por exemplo, contra perda de confidencialidade, uso indevido ou perda de integridade).

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Para o controle da informação documentada, a organização deve considerar as seguintes atividades, conforme aplicadas:

a) distribuição, acesso, recuperação e uso;

b) armazenagem e preservação, incluindo a preservação da legibilidade;

c) controle de mudanças (por exemplo, controle de versão);

d) retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e operação do sistema de gestão da segurança da informação, deve ser identificada como apropriado, e controlada.

NOTA O acesso implica em uma decisão quanto à permissão para apenas ler a informação documentada ou a permissão e autoridade para ver e alterar a informação documentada.

8 Operação

8.1 Planejamento operacional e controle

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos de segurança da informação e para implementar as ações determinadas em 6.1. A organização deve também implementar planos para alcançar os objetivos de segurança da informação determinados em 6.2.

A organização deve manter a informação documentada na abrangência necessária para gerar confiança de que os processos estão sendo realizados conforme planejado.

A organização deve controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não previstas, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

A organização deve assegurar que os processos terceirizados estão determinados e são controlados.

8.2 Avaliação de riscos de segurança da informação

A organização deve realizar avaliações de riscos de segurança da informação a intervalos planejados, ou quando mudanças significativas são propostas ou ocorrem, levando em conta os critérios estabelecidos em 6.1.2 a).

A organização deve reter informação documentada dos resultados das avaliações de risco de segurança da informação.

8.3 Tratamento de riscos de segurança da informação

A organização deve implementar o plano de tratamento de riscos de segurança da informação.

A organização deve reter informação documentada dos resultados do tratamento dos riscos de segurança da informação.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

9 Avaliação do desempenho

9.1 Monitoramento, medição, análise e avaliação

A organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão da segurança da informação.

A organização deve determinar:

a) o que precisa ser monitorado e medido, incluindo controles e processos de segurança da informação;

b) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

NOTA Recomenda-se que os métodos selecionados produzam resultados comparáveis e reproduzíveis para serem válidos.

c) quando o monitoramento e a medição devem ser realizados;

d) o que deve ser monitorado e medido;

e) quando os resultados do monitoramento e da medição devem ser analisados e avaliados;

f) quem deve analisar e avaliar estes resultados.

A organização deve reter informação documentada apropriada como evidência do monitoramento e dos resultados da medição.

9.2 Auditoria interna

A organização deve conduzir auditorias internas a intervalos planejados para prover informações sobre o quanto o sistema de gestão da segurança da informação:

a) está em conformidade com:

   1) os próprios requisitos da organização para o seu sistema de gestão da segurança da informação;

   2) os requisitos desta Norma;

b) está efetivamente implementado e mantido.

A organização deve:

a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores;

b) definir os critérios e o escopo da auditoria, para cada auditoria;

c) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

d) assegurar que os resultados das auditorias são relatados para a direção pertinente.

e) reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria.

9.3 Análise crítica pela Direção

A Alta Direção deve analisar criticamente o sistema de gestão da segurança da informação da organização a intervalos planejados, para assegurar a sua contínua adequação, pertinência e eficácia.

A análise crítica pela Direção deve incluir considerações com relação a:

a) situação das ações de análises críticas anteriores, realizadas pela Direção;

b) mudanças nas questões internas e externas, que sejam relevantes para o sistema de gestão da segurança da informação;

c) realimentação sobre o desempenho da segurança da informação, incluindo tendências em:

   1) não conformidades e ações corretivas;

   2) monitoramento e resultados da medição;

   3) resultados de auditorias; e

   4) cumprimento dos objetivos de segurança da informação;

d) realimentação das partes interessadas;

e) resultados da avaliação dos riscos e situação do plano de tratamento dos riscos; e

f) oportunidades para melhoria contínua.

Os resultados da análise crítica pela Direção devem incluir decisões relativas a oportunidades para melhoria contínua e quaisquer necessidades para mudanças do sistema de gestão da segurança da informação.

A organização deve reter informação documentada como evidência dos resultados das análises críticas pela Direção.

10 Melhoria

10.1 Não conformidade e ação corretiva

Quando uma não conformidade ocorre, a organização deve:

a) reagir a não conformidade e, conforme apropriado:

   1) tomar ações para controlar e corrigi-la; e

   2) tratar com as consequências;

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

b) avaliar a necessidade de ações para eliminar as causas de não conformidade, para evitar sua repetição ou ocorrência, por um dos seguintes meios:

   1) analisando criticamente a não conformidade;

   2) determinando as causas da não conformidade; e

   3) determinando se não conformidades similares existem, ou podem potencialmente ocorrer.

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas; e

e) realizar mudanças no sistema de gestão da segurança da informação, quando necessário.

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas.

A organização deve reter informação documentada como evidência da:

a) natureza das não conformidades e quaisquer ações subsequentes tomadas; e

b) resultados de qualquer ação corretiva.

10.2 Melhoria contínua

A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Anexo A
(normativo)

Referência aos controles e objetivos de controles

Os controles e objetivos de controles listados na Tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013 [1], Seções 5 a 18, e devem ser usados em alinhamento com 6.1.3

Tabela A.1 – Objetivos de controle e controles

A.5 Políticas de segurança da informação		
A.5.1 Orientação da Direção para segurança da informação		
Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Políticas para segurança da informação	*Controle* Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica das políticas para segurança da informação	*Controle* As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
A.6 Organização da segurança da informação		
A.6.1 Organização interna		
Objetivo: Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.		
A.6.1.1	Responsabilidades e papéis da segurança da informação	*Controle* Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas.
A.6.1.2	Segregação de funções	*Controle* Funções conflitantes e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.
A.6.1.3	Contato com autoridades	*Controle* Contatos apropriados com autoridades relevantes devem ser mantidos.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.6 Organização da segurança da informação		
A.6.1 Organização interna		
Objetivo: Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.		
A.6.1.4	Contato com grupos especiais	*Controle* Contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação devem ser mantidos.
A.6.1.5	Segurança da informação no gerenciamento de projetos	*Controle* Segurança da informação deve ser considerada no gerenciamento de projetos, independentemente do tipo do projeto.
A.6.2 Dispositivos móveis e trabalho remoto.		
Objetivo: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis		
A.6.2.1	Política para o uso de dispositivo móvel	*Controle* Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.
A.6.2.2	Trabalho remoto	*Controle* Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.
A.7 Segurança em recursos humanos		
A.7.1 Antes da contratação		
Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.		
A.7.1.1	Seleção	*Controle* Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
A.7.1.2	Termos e condições de contratação	*Controle* As obrigações contratuais com funcionários e partes externas devem declarar a sua responsabilidade e a da organização para a segurança da informação

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.7.2 Durante a contratação		
Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.		
A.7.2.1	Responsabilidades da Direção	*Controle* A Direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
A.7.2.2	Conscientização, educação e treinamento em segurança da informação	*Controle* Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.
A.7.2.3	Processo disciplinar	*Controle* Deve existir um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.
A.7.3 Encerramento e mudança da contratação		
Objetivo: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.		
A.7.3.1	Responsabilidades pelo encerramento ou mudança da contratação	*Controle* As responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação devem ser definidas, comunicadas aos funcionários ou partes externas e cumpridas.
A.8 Gestão de ativos		
A.8.1. Responsabilidade pelos ativos		
Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.		
A.8.1.1	Inventário dos ativos	*Controle* Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido.
A.8.1.2	Proprietário dos ativos	*Controle* Os ativos mantidos no inventário devem ter um proprietário.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.8 Gestão de ativos		
A.8.1. Responsabilidade pelos ativos		
Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.		
A.8.1.3	Uso aceitável dos ativos	*Controle* Regras para o uso aceitável das informações, dos ativos associados com informação e os recursos de processamento da informação devem ser identificados, documentados e implementados.
A.8.1.4	Devolução de ativos	*Controle* Todos os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.
A.8.2 Classificação da informação		
Objetivo: Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.		
A.8.2.1	Classificação da informação	*Controle* A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
A.8.2.2	Rótulos e tratamento da informação	*Controle* Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.
A.8.2.3	Tratamento dos ativos	*Controle* Procedimentos para o tratamento dos ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.
A.8.3 Tratamento de mídias		
Objetivo: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.		
A.8.3.1	Gerenciamento de mídias removíveis	*Controle* Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.8.3.2	Descarte de mídias	*Controle* As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
A.8.3.3	Transferência física de mídias	*Controle* Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.
A.9 Controle de acesso		
A.9.1 Requisitos do negócio para controle de acesso		
Objetivo: Limitar o acesso à informação e aos recursos de processamento da informação.		
A.9.1.1	Política de controle de acesso	*Controle* Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
A.9.1.2	Acesso às redes e aos serviços de rede	*Controle* Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
A.9.2 Gerenciamento de acesso do usuário		
Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.		
A.9.2.1	Registro e cancelamento de usuário	*Controle* Um processo formal de registro e cancelamento de usuário deve ser implementado para permitir atribuição dos direitos de acesso.
A.9.2 Gerenciamento de acesso do usuário		
Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.		
A.9.2.2	Provisionamento para acesso de usuário	*Controle* Um processo formal de provisionamento de acesso do usuário deve ser implementado para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.9.2.3	Gerenciamento de direitos de acesso privilegiado	*Controle* A concessão e uso de direitos de acesso privilegiado devem ser restritos e controlados.
A.9.2.4	Gerenciamento da informação de autenticação secreta de usuários	*Controle* A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal.
A.9.2.5	Análise crítica dos direitos de acesso do usuário	*Controle* Os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários, a intervalos regulares.
A.9.2.6	Retirada ou ajuste dos direitos de acesso	*Controle* Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.
A.9.3 Responsabilidades dos usuários		
Objetivo: Tornar os usuários responsáveis pela proteção das suas informações de autenticação.		
A.9.3.1	Uso da informação de autenticação secreta	*Controle* Os usuários devem ser orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.
A.9.4 Controle de acesso ao sistema e à aplicação		
Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.		
A.9.4.1	Restrição de acesso à informação	*Controle* O acesso à informação e às funções dos sistemas de aplicações deve ser restrito de acordo com a política de controle de acesso.
A.9.4.2	Procedimentos seguros de entrada no sistema (*log-on*)	*Controle* Onde aplicavél pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (*log-on*).
A.9.4.3	Sistema de gerenciamento de senha	*Controle* Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.9.4.4	Uso de programas utilitários privilegiados	*Controle* O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.
A.9.4.5	Controle de acesso ao código-fonte de programas	*Controle* O acesso ao código-fonte de programa deve ser restrito.
A.10 Criptografia		
A.10.1 Controles criptográficos		
Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.		
A.10.1.1	Política para o uso de controles criptográficos	*Controle* Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
A.10.1.2	Gerenciamento de chaves	*Controle* Uma política sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida.
A.11 Segurança física e do ambiente		
A.11.1 Áreas seguras		
Objetivo: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.		
A.11.1.1	Perímetro de segurança física	*Controle* Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.
A.11.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
A.11.1.3	Segurança em escritórios, salas e instalações	*Controle* Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.11.1.4	Proteção contra ameaças externas e do meio ambiente	*Controle* Deve ser projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes.
A.11.1.5	Trabalhando em áreas seguras	*Controle* Devem ser projetados e aplicados procedimentos para o trabalho em áreas seguras.
A.11.1.6	Áreas de entrega e de carregamento	*Controle* Pontos de acesso, como áreas de entrega e de carregamento, e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.
A.11.2 Equipamentos		
Objetivo: Impedir perdas, danos, roubo, ou comprometimento de ativos e interrupção das operações da organização.		
A.11.2.1	Localização e proteção do equipamento	*Controle* Os equipamentos devem ser protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
A.11.2 Equipamentos		
Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.		
A.11.2.2	Utilidades	*Controle* Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
A.11.2.3	Segurança do cabeamento	*Controle* O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos.
A.11.2.4	Manutenção dos equipamentos	*Controle* Os equipamentos devem ter uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.11.2.5	Remoção de ativos	*Controle* Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.
A.11.2.6	Segurança de equipamentos e ativos fora das dependências da organização	*Controle* Devem ser tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
A.11.2.7	Reutilização e ou descarte seguro de equipamentos	*Controle* Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.
A.11.2.8	Equipamento de usuário sem monitoração	*Controle* Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
A.11.2.9	Política de mesa limpa e tela limpa	*Controle* Devem ser adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
A.12 Segurança nas operações		
A.12.1 Responsabilidades e procedimentos operacionais		
Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.		
A.12.1.1	Documentação dos procedimentos de operação	*Controle* Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitam deles.
A.12.1.2	Gestão de mudanças	*Controle* Mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação devem ser controladas.
A.12.1.3	Gestão de capacidade	*Controle* A utilização dos recursos deve ser monitorada e ajustada, e as projeções devem ser feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.12.1.4	Separação dos ambientes de desenvolvimento, teste e de produção	*Controle* Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
A.12.2 Proteção contra *malware*		
Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*.		
A.12.2.1	Controles contra malware	*Controle* Devem ser implementados controles de detecção, prevenção e recuperação para proteger contra *malware*, combinados com um adequado programa de conscientização do usuário.
A.12.3 Cópias de segurança		
Objetivo: Proteger contra a perda de dados.		
A.12.3.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações, *softwares* e das imagens do sistema devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
A.12.4 Registros e monitoramento		
Objetivo: Registrar eventos e gerar evidências.		
A.12.4.1	Registros de eventos	*Controle* Registros de eventos (*log*) das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares
A.12.4.2	Proteção das informações dos registros de eventos (*logs*)	*Controle* As informações dos registros de eventos (*log*) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.
A.12.4.3	Registros de eventos (*log*) de administrador e operador	*Controle* As atividades dos administradores e operadores do sistema devem ser registradas e os registros (*logs*) devem ser protegidos e analisados criticamente, a intervalos regulares.
A.12.4.4	Sincronização dos relógios	*Controle* Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.12.5 Controle de *software* operacional		
Objetivo: Assegurar a integridade dos sistemas operacionais.		
A.12.5.1	Instalação de *software* nos sistemas operacionais	*Controle* Procedimentos para controlar a instalação de *software* em sistemas operacionais devem ser implementados.
A.12.6 Gestão de vulnerabilidades técnicas		
Objetivo: Prevenir a exploração de vulnerabilidades técnicas.		
A.12.6.1	Gestão de vulnerabilidades técnicas	*Controle* Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas em tempo hábil; a exposição da organização a estas vulnerabilidades deve ser avaliada e devem ser tomadas as medidas apropriadas para lidar com os riscos associados.
A.12.6.2	Restrições quanto à instalação de *software*	*Controle* Regras definindo critérios para a instalação de *software* pelos usuários devem ser estabelecidas e implementadas.
A.12.7 Considerações quanto à auditoria de sistemas de informação		
Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.		
A.12.7.1	Controles de auditoria de sistemas de informação	*Controle* As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negócio.
A.13 Segurança nas comunicações		
A.13.1 Gerenciamento da segurança em redes		
Objetivo: Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.		
A.13.1.1	Controles de redes	*Controle* As redes devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
A.13.1.2	Segurança dos serviços de rede	*Controle* Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.13.1.3	Segregação de redes	*Controle* Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.
A.13.2 Transferência de informação		
Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.		
A.13.2.1	Políticas e procedimentos para transferência de informações	*Controle* Políticas, procedimentos e controles de transferências formais devem ser estabelecidos para proteger a transferência de informações por meio do uso de todos os tipos de recursos de comunicação.
A.13.2.2	Acordos para transferência de informações	*Controle* Devem ser estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.
A.13.2 Transferência de informação		
Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.		
A.13.2.3	Mensagens eletrônicas	*Controle* As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
A.13.2.4	Acordos de confidencialidade e não divulgação	*Controle* Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados, analisados criticamente e documentados.
A.14 Aquisição, desenvolvimento e manutenção de sistemas		
A.14.1 Requisitos de segurança de sistemas de informação		
Objetivo: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.		
A.14.1.1	Análise e especificação dos requisitos de segurança da informação	*Controle* Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.14.1.2	Serviços de aplicação seguros em redes públicas	*Controle* As informações envolvidas nos serviços de aplicação que transitam em redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
A.14.1.3	Protegendo as transações nos aplicativos de serviços	*Controle* Informações envolvidas em transações nos aplicativos de serviços devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
A.14.2 Segurança em processos de desenvolvimento e de suporte		
Objetivo: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.		
A.14.2.1	Política de desenvolvimento seguro	*Controle* Regras para o desenvolvimento de sistemas e *software* devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.
A.14.2.2	Procedimentos para controle de mudanças de sistemas	*Controle* Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças.
A.14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	*Controle* Aplicações críticas de negócios devem ser analisadas criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
A.14.2.4	Restrições sobre mudanças em pacotes de *software*	*Controle* Modificações em pacotes de *software* devem ser desencorajadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.
A.14.2.5	Princípios para projetar sistemas seguros	*Controle* Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.14.2.6	Ambiente seguro para desenvolvimento	*Controle* As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema
A.14.2.7	Desenvolvimento terceirizado	*Controle* A organização deve supervisionar e monitorar as atividades de desenvolvimento de sistemas terceirizado.
A.14.2 Segurança em processos de desenvolvimento e de suporte		
Objetivo: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.		
A.14.2.8	Teste de segurança do sistema	*Controle* Testes de funcionalidade de segurança devem ser realizados durante o desenvolvimento de sistemas.
A.14.2.9	Teste de aceitação de sistemas	*Controle* Programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões.
A.14.3 Dados para teste		
Objetivo: Assegurar a proteção dos dados usados para teste.		
A.14.3.1	Proteção dos dados para teste	*Controle* Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.
A.15 Relacionamento na cadeia de suprimento		
A.15.1 Segurança da informação na cadeia de suprimento		
Objetivo: Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.		
A.15.1.1	Política de segurança da informação no relacionamento com os fornecedores	*Controle* Requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização devem ser acordados com o fornecedor e documentados.
A.15.1.2	Identificando segurança da informação nos acordos com fornecedores	*Controle* Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.15.1.3	Cadeia de suprimento na tecnologia da informação e comunicação	*Controle* Acordos com fornecedores devem incluir requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação.
A.15.2 Gerenciamento da entrega do serviço do fornecedor		
Objetivo: Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.		
A.15.2.1	Monitoramento e análise crítica de serviços com fornecedores	*Controle* A organização deve monitorar, analisar criticamente e auditar, a intervalos regulares, a entrega dos serviços executados pelos fornecedores.
A.15.2.2	Gerenciamento de mudanças para serviços com fornecedores	*Controle* Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos e a reavaliação de riscos.
A.16 Gestão de incidentes de segurança da informação		
A.16.1 Gestão de incidentes de segurança da informação e melhorias		
Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.		
A.16.1.1	Responsabilidades e procedimentos	*Controle* Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.
A.16.1.2	Notificação de eventos de segurança da informação	*Controle* Os eventos de segurança da informação devem ser relatados por meio dos canais de gestão, o mais rapidamente possível.
A.16.1.3	Notificando fragilidades de segurança da informação	*Controle* Os funcionários e partes externas que usam os sistemas de informação e serviços da organização devem ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.16.1.4	Avaliação e decisão dos eventos de segurança da informação	*Controle* Os eventos de segurança da informação devem ser avaliados, e deve ser decidido se eles são classificados como incidentes de segurança da informação.
A.16 Gestão de incidentes de segurança da informação		
A.16.1 Gestão de incidentes de segurança da informação e melhorias		
Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.		
A.16.1.5	Resposta aos incidentes de segurança da informação	*Controle* Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados.
A.16.1.6	Aprendendo com os incidentes de segurança da informação	*Controle* Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação devem ser usados para reduzir a probabilidade ou o impacto de incidentes futuros.
A.16.1.7	Coleta de evidências	*Controle* A organização deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.
A.17 Aspectos da segurança da informação na gestão da continuidade do negócio		
A.17.1 Continuidade da segurança da informação		
Objetivo: A continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização.		
A.17.1.1	Planejando a continuidade da segurança da informação	*Controle* A organização deve determinar seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.
A.17.1.2	Implementando a continuidade da segurança da informação	*Controle* A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	*Controle* A organização deve verificar os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.
A.17.2 Redundâncias		
Objetivo: Assegurar a disponibilidade dos recursos de processamento da informação.		
A.17.2.1	Disponibilidade dos recursos de processamento da informação	*Controle* Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.
A.18 Conformidade		
A.18.1 Conformidade com requisitos legais e contratuais		
Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.		
A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais	*Controle* Todos os requisitos legislativos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.
A.18.1.2	Direitos de propriedade intelectual	*Controle* Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.
A.18.1.3	Proteção de registros	*Controle* Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
A.18.1.4	Proteção e privacidade de informações de identificação de pessoal	*Controle* A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Tabela A.1 (continuação)

A.18.1.5	Regulamentação de controles de criptografia	*Controle* Controles de criptografia devem ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.
A.18.2 Análise crítica da segurança da informação		
Objetivo: Assegurar que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.		
A.18.2.1	Análise crítica independente da segurança da informação	*Controle* O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.
A.18.2.2	Conformidade com as políticas e normas de segurança da informação	*Controle* Os gestores devem analisar criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.
A.18.2.3	Análise crítica da conformidade técnica	*Controle* Os sistemas de informação devem ser analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados

Bibliografia

[1] ABNT NBR ISO IEC 27002:2013, *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*

[2] ABNT NBR ISO IEC 27003, *Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação*

[3] ABNT NBR ISO/IEC 27004, *Tecnologia da informação – Técnicas de segurança – Gestão da segurança da informação – Medição*

[4] ABNT NBR ISO/IEC 27005, *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação*

[5] ABNT NBR ISO 31000:2009, *Gestão de riscos – Princípios e diretrizes*

[6] ISO IEC Directives, Part 1 *Consolidated ISO Supplement – Procedures specific to* ISO:2012

© ISO/IEC 2013 - © ABNT 2013 - Todos os direitos reservados